BY ORDER OF THECOMMANDER
FOURTH AIR FORCE

FOURTH AIR FORCE INSTRUCTION 33-202

13 August 1999

Communications and Information

UNITED STATES AIR FORCE RESERVE COMMAND (AFRC) INTRUSION DETECTION SYSTEM – RESPONSE PROCEDURES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFRC WWW site at: http://www.afrc.af.mil and the AFRCEPL (CD-ROM) published monthly.

OPR: 604 RSG/SC (TSgt Michael Hollinshead) Certified by: 4AF/CVA (Col Thomas M. Gisler, Jr.)
Pages: 4
Distribution: F

This instruction implements AFPD 33-2, *Information Protection*, and AFPD 31-4, *Information Security*. The purpose of this instruction is to detail 4th Air Force response procedures in the event of alarm activation for the Secure Internet Protocol Router Network (SIPRNET)/Global Command and Control System (GCCS). It defines personnel responsible for recall procedures and processes if the alarm activation occurs indicating a possible security breach. This procedure applies to all personnel of this Headquarters, 604 Regional Support Group (604 RSG), and 904 Civil Engineering Squadron (904 CES).

1. General Concept. The SIPRNET/GCCS network provides classified e-mail and information technology applications to selective identified staff of 4th Air Force personnel based on the individual's security clearance and a need-to-know. This network is the cornerstone of our ability to properly engage and manage Command, Control, Communications, and Information (C4I) applications and processes. The system is currently accredited and approved to process e-mail traffic and Information Technology applications up to and including Secret level.

1.1. The 4th Air Force SIPRNET circuit connection is initiated in the 452nd Communications Squadron (Bldg. 2404) and connects to the 4th Air Force Operations Center (Bldg. 323/Room 200). The SIPRNET connection in Bldg. 323 then branches out to the 4th Air Force Intelligence Office (Bldg. 323/Room 204) and the 4th Air Force Plans and Programs Office (Bldg. 323/Room 206A2-3). The SIPRNET line that connects all three 4th Air Force stations runs above the ceiling via a Protected Distribution System. The alarm system is a Commercial Off-the-Shelf (COTS) variety and installed by a commercial vendor. The alarm is tied into the current existing 4th Air Force Operations Center and the main base Security Forces monitoring system. 452nd Security Forces monitor the system on a 24-hour basis.

2. Terms Explained:

2.1. Global Command and Control System (GCCS) - The secure/classified C4I system used to process and disseminate classified material.

2.2. Installation SIPRNET Security Officer (ISSO) - The primary point of contact (POC) for all GCCS security-related issues, processes, and procedures within 4th Air Force. The ISSO will serve as the primary responder to all security alarms/recalls for the 4th Air Force SIPRNET/GCCS program. The ISSO is designated in writing by the 4 AF/CC to the host base, HQ AFRC GCCS office, and the Defense Information System Agency (DISA).

2.3. Secure Internet Protocol Router Network (SIPRNET) - The current medium in which the secure/classified traffic passes from one GCCS terminal to another.

2.4. Security Response - A response by personnel (e.g. designated 4th Air Force personnel, 452nd Security Forces, 452nd Communications Squadron, etc.) to a security alarm/breach.

2.5. Section Security Manager - Personnel designated by Division Chief(s) responsible for all security aspects of section GCCS processes and procedures.

3. Responsibilities:

3.1. The commander will designate the 4th Air Force ISSO in writing.

3.2. The ISSO will establish, implement, and manage a security program for 4th Air Force secure/classified Information Technology applications.

3.2.1. The ISSO will serve as the POC for all security issues pertaining to 4th Air Force secure/classified Information Technology applications.

3.3. The ISSO (or designated representative) will serve as the first/primary responder for any recalls concerning the SIPRNET/GCCS alarm system.

3.3.1. After responding to an active alarm, the ISSO will ascertain the situation, act as the on-scene commander, and recall appropriate section security managers and/or 452CS/GCCS personnel as required.

3.3.2. Section security managers will respond to ISSO recalls and secure GCCS section work stations/areas as required. If no response by the section security manager, the ISSO will contact base Security Forces to conduct facility checks every 2 hours. The ISSO will up/cross-channel all security incident reports as required by AFI 31-401 and supplements.

3.3.3. The ISSO (in coordination with host base GCCS and Security Forces managers) will provide section security training and assistance visits to ensure the validity of 4th Air Force programs.

3.3.4. The ISSO will coordinate with host base agencies (e.g. Security Forces, CES, SC, etc.) to test existing alarm systems at least on a quarterly basis and report test results accordingly.

3.4. Division Chiefs will appoint section security managers (primary and alternate) in writing to the 4th Air Force ISSO.

3.4.1. Section Security managers will be responsible for GCCS system security within their respective section and work area.

3.4.2. Section security managers will coordinate/schedule training, assistance visits, and alarm testing with the 4th Air Force ISSO.

3.4.3. Section security managers will be responsible for responding to section GCCS alarms when recalled by the 4th Air Force ISSO.

3.4.4. Section security managers will ensure all visitors to the GCCS terminal area are signed in using AF Form 1109, **Visitor Register Log**, and properly escorted.

3.4.5. Section security managers will modify existing SF 701, **Activity Security Checklist**, and area checklist(s) to include GCCS security procedures (e.g. removal and storage of the classified hard drive, securing work station areas when GCCS is in use, conducting GCCS software/hardware inventory, etc.). Section managers will incorporate existing disaster plans.

3.4.5.1. Perform section/work area security inspections as required (normally last person working on GCCS terminal will be responsible for end-of-day security).

3.4.5.2. Immediately report any security violations to the division chief and the ISSO (not necessarily in that order).

3.4.5.3. In case of an emergency (e.g. fire, natural disaster, etc.) take all actions necessary to secure/remove/destroy classified materials if events/time permits (e.g. remove the classified hard drive and take it with you). Establish an internal security recovery plan for your section. Procedures for protection, removal, or destruction of classified material must be adhered to in the event of:

3.4.5.3.1. Fire. All classified material will be returned to the security container, if possible, and the container locked. If the material cannot be returned to the security container, the person possessing the material will maintain custody until relieved or the material is secured in an approved security container. If the classified material cannot be removed from the building or the security container cannot be locked, the Fire Chief will be notified immediately. When the Fire Chief declares the area safe, all classified material or its remains will be secured and the ISPM notified immediately.

3.4.5.3.2. Natural Disaster. Earthquake can occur without warning. Upon receiving warning of a tornado or severe weather, all classified material that is not absolutely mission essential should be placed in the security container and the container locked. If the classified material or security container is destroyed, scattered, or spirited away by natural forces, every effort will be made to find and secure the material or its remains and contact the ISPM for additional guidance. Should a container be found following a severe storm or earthquake that damages the base and building housing containers, contact the ISPM, who maintains a listing of containers.

3.4.5.3.3. Civil Disturbance. All agencies will normally be warned in advance. However should a disturbance occur without warning, all classified material will be returned to the security container immediately and the container locked. The unit commander or staff agency chief will determine if any additional protection is needed.

3.4.5.3.4. Evacuation. The installation commander may direct that all classified material be evacuated from March Air Reserve Base. Regardless of the method used, personnel will ensure that all classified material is bagged, boxed, or crated and sealed as appropriate IAW DOD 5200.1-R. An AF 310, **Document Receipt and Destruction Certificate** will be accomplished indicating the number of containers, and the highest classification level of material contained inside and the identity of the sending unit. An Evacuation Officer

will be appointed by 604RSG/CC and will sign for each container.

3.4.5.4. Establish/delete GCCS account processes as required. Perform section security training as required.

4. Procedures:

4.1. The SIPRNET/GCCS alarm will be monitored on a 24-hour basis by 452nd Security Forces Central Station.

4.1.1. During normal duty hours, the responding Security Forces will coordinate with the ISSO to determine validity of alarm and then take appropriate actions as required.

4.1.2. After normal duty hours, responding Security Forces will do a visual inspection of GCCS alarmed facilities to determine any breaches of security. If Security Forces determine that the building is secured and the alarm can be successfully reset by Security Forces Central Monitoring Station, Security Forces will log the event as a false alarm and contact the ISSO.

4.1.2.1. If responding Security Forces find/determine a physical breach of the building/GCCS alarm system, they will immediately secure the area and recall the 4th Air Force ISSO. Upon arrival, the ISSO will serve as the 4th Air Force on-scene commander, take all actions necessary to secure the breach, and recall security managers as required to secure individual areas. The 4th Air Force ISSO will coordinate with host base GCCS managers to immediately terminate all SIPRNET connectivity until system security can be revalidated.

4.2. All scheduled/unscheduled above-the-ceiling maintenance (e.g. air conditioner, electric phone, etc.) will be coordinated with the 4th Air Force ISSO and the building custodian prior to commencement.

4.3. Line inspections will be conducted on a monthly schedule and documented by the ISSO. Each year there will be a technical inspection conducted by the ISSO to ensure the conduit meets all security requirements.

4.4. An alarm test will be conducted each quarter to insure the Intrusion Detection System is working properly and results will be documented on AF Form 2530, **Alarm System Test Record**. Ensure the security police desk is notified prior to any alarm testing.

WALLACE W. WHALEY, Maj Gen, USAFR
Commander